AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Seven Electronic Devices Identified in Attachment A and located at 9221 Public Works Road, Chesterfield, VA

3:18SW134

Case No. UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment A, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 1344	Bank Fraud
18 U.S.C. 1028A	Aggravated Identity Theft

The application is based on these facts:

See Attached Affidavit, incorporated herein by reference

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

Heather Hart Mansfield

TFO
Applicant's signature

Michael S. Bowser, TFO United States Secret Service
Printed name and title

Sworn to before me and signed in my presence.

/s/
David J. Novak
United States Magistrate Judge
Judge's signature

Date: May 29, 2018

City and state: Richmond, Virginia

David J. Novak, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Richmond Division

IN THE MATTER OF THE SEARCH OF FOLLOWING DEVICES: Black ZTE cell phone, model Sky MM8005, S/N 325769982688; Red and white iPhone, model 1660, FCC ID BCG-E3085A, cracked screen; White iPhone S, Model A 1688, FFC ID BCG-E2946A, cracked screen; Black Dell Laptop, Model P28F, S/N 276662519917; Gray HP Laptop with purple diamond sticker, Model 2000-369WM, S/N 53B218W2Y; Black IST Discover Flash Drive; Black Coolpad Cellphone – Model 5560S,MEID (DEC) – 256691536606894695, MEID (HEX) – 99000526693467, cracked screen; Black iPhone – Model A1784, FCC ID: BCG-E3092A, IC: 579C-E3092A, cracked screen LOCATED AT 9221 Public Works Road, Chesterfield, VA 23832.	**UNDER SEAL** Case No. 3:18sw134

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Michael Scot Bowser, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—that is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Detective with the Chesterfield County Police Department (CCPD). I have been employed by CCPD since September 2001, and have been a Detective since December 2007. I am currently assigned to the Economic Crimes Unit, Criminal Investigations Division, and I am a Task Force Officer with the Metro Richmond Identity Theft Task Force. I have conducted investigations of check fraud, identity theft, and access device fraud cases. I have participated in the preparation and presentation of arrest warrants and search warrants related to fraud investigations, and I am familiar with the methods of individuals who use social media, cellular phones, and computers to commit bank fraud.

3. Since October 2017, I have been deputized as a United States Marshal. As such, I am authorized to investigation violations of the laws of the United States and am a law enforcement officer with authority to execute warrants under the authority of the United States.]

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is:

   a. A Black ZTE cell phone, model Sky MM8005, S/N 325769982688, hereinafter "Device 1";

   b. A Red and white iPhone Model 1660 FCC ID BCG-E3085A, cracked screen, hereinafter "Device 2",

c. White iPhone S Model A 1688 FFC ID BCG-E2946A, cracked screen, hereinafter "Device 3",

d. Black Dell Laptop Model P28F S/N 276662519917, hereinafter "Device 4",

e. an Gray HP Laptop with purple diamond sticker, Model 2000-369WM, S/N 53B218W2Y, hereinafter "Device 5",

f. and a Black IST Discover Flash Drive, hereinafter "Device 6."

g. Black Coolpad Cellphone – Model 5560S,MEID (DEC) 256691536606894695, MEID (HEX) – 99000526693467, cracked screen, hereinafter "Device 7",

h. Black iPhone – Model A1784, FCC ID: BCG-E3092A, IC: 579C-E3092A, cracked screen, hereinafter "Device 8."

6. The Devices are currently located at the Chesterfield County Police Department's Property and Evidence Building, located at 9221 Public Works Road Chesterfield, VA 23832.

7. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

RELEVANT STATUTORY PROVISIONS

8. Bank Fraud: 18 U.S.C. § 1344 makes it a violation of federal law to knowingly execute, or attempt to execute, a scheme or artifice to defraud a financial institution or to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises.

9. Aggravated Identity Theft: 18 U.S.C. § 1028A prohibits anyone, who during and in relation to any felony violation enumerated in subsection (c), which section includes Bank

Fraud, in violation of 18 U.S.C. § 1344, from knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person.

10.

TECHNICAL TERMS

11. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. **Wireless telephone**: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. **Flash Drive**: A small, data storage device used to store files or transport them from one computer to another, also commonly referred to as a USB or thumb drive.

c. The term "**computer / tablet**" as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

d. The terms "**records**," "**documents**," and "**materials**," include all information recorded in any form, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following: Graphic records or representations, photographs, pictures, images, and aural records or representations.

e. **IP Address**: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

f. **Internet**: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

12. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at http://www.apple.com., http://www.hp.com, http://www.dell.com, and http://www.istdiscover-e.com, http://www.zteusa.com, and http://coolpad.us. I know that Devices 1,2,3,7, and 8 are cell phones, which are handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. Devices 4 and 5 are computers, and Device 6 is a flash drive, all defined above.

13. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

PROBABLE CAUSE

14. On September 12, 2017, Officer Morgan, CCPD, was dispatched to 5753 Quiet Pine Circle, Apartment 302, Chester, VA 23831 in reference to a shooting. When Officer Morgan approached the building, he noticed water running down the side of the building. Officer Morgan spoke with the occupant of Apartment 304, who advised he believed the gunshot came from Apartment 302.

15. Officer Morgan and Officer Lombardo made entry into Apartment 302 to ensure no one was injured or trapped inside. Upon entry, Officer Morgan observed that a water line had been struck by a bullet, causing water to come out of the pipe. While clearing the apartment, Officer Morgan saw marijuana in plain view on a table in the living room. Officer Lombardo then secured the scene while a search warrant was being obtained.

16. While on scene, Officer Morgan spoke with witnesses at the apartment complex regarding the reports of gunfire. One such witness was J.R. J.R. stated that she was inside Apartment 302 when the pipe was shot. J.R. initially advised that there was no gunfire from inside the apartment. After Officer Morgan questioned this story, J.R. stated that the male in the apartment, later identified as William Reed, was cleaning a gun when it accidently discharged.

17. William Reed, along with another individual, is the leaseholder of Apartment 302.

18. Officers obtained a search warrant from the Chesterfield County Magistrate's Office to search the apartment for marijuana and firearms based on their observation of marijuana in plain view. During this search, officers discovered thousands of dollars on the fireplace and in a drawer in the kitchen, beside the refrigerator. Officer Morgan also located a magnetic card reader inside the hallway closet and several identifications and credit/debit cards in the apartment that did not belong to William Reed or J.R.

19. After discovering these items, Officer Morgan recognized these items as potential evidence of identity theft and fraud. He stopped the search and obtained an additional search warrant from the Chesterfield County Magistrate's Office for credit/debit cards, documents of identification, electronic devices, including cell phones, flash drives, hard drives, SIM cards, magnetic strip readers, and programmers, and any other electronic storage devices.

20. During the execution of these search warrants, several additional items were confiscated from Apartment 302, including: 22 counterfeit hundred-dollar bills; 13 legal documents belonging to William Reed; 1 hand written document containing forged signatures of various people; 13 identification cards that did not match the identity of William Reed or J.R.; 14 debit cards in the name of other individuals, not William Reed or J.R.; a box of check paper from Amazon mailed to William Reed; fraudulent checks; and a magnetic card reader.

21. Devices 1, 2, 3, 4, 6, 7, and 8 were also located during the search of Apartment 302.

22. Officer Morgan obtained warrants for William Reed for Credit Card Theft and Fraudulent Use of Birth Certificates, etc. William Reed was arrested on September 13, 2017, by Henrico County Police and transferred to the custody of the Chesterfield County Police Department.

23. On September 13, 2017, Detective Bates, CCPD, obtained a search warrant for William Reed's mother's house, located in Chesterfield, VA. Detectives had information that Reed also stayed in that location. During this search, counterfeit bills and a cell phone belonging to Reed were seized during that search. Additionally, Device 5 was located at this residence in a room identified being used by Reed.

24. On September 15, 2017, Detective Bates obtained a search warrant for William Reed's cell phone, which was recovered in the September 13 search of his mother's home. The search warrant was executed and data was recovered from the phone. William Reed had numerous text messages and chat messages on his phone pertaining to card cracking. Several different individuals messaged with William Reed and gave Reed bank account numbers, the associated pin numbers, and the online banking login and passwords associated with the accounts. There are pictures of bank statements and bank cards belonging to other individuals stored on William Reed's phone. Additionally, pictures of money orders and checks showing the routing numbers are on William Reed's phone. Detective Bates issued subpoenas for many of the bank accounts found in text messages on William Reed's phone and found fraudulent activity on the accounts involving the deposits of fraudulent checks.

25. Based on my training and experience, the evidence found on Reed's phone demonstrates that he used his phone and social media to recruit and solicit individuals who possessed current bank accounts. These recruited account holders – "recruits" – would subsequently agree to provide their ATM cards and corresponding Personal Identification Numbers ("PINs") in exchange for payment. Once in possession of the banking information and PINs, REED or other individuals he recruited would deposit stolen or fraudulent checks into those accounts and then withdraw the available funds from the recruit's account before the financial institution was aware that the deposited funds were fraudulent or stolen.

26. Checks can be created using computer software programs such as VersaCheck and Checksoft, which are readily available for purchase at local stores or online, and which can be used on a personal computer. Checks can be customized and personalized and then easily printed on blank check stock using simple inkjet printers. In the type of fraud described above,

the initial step is typically to obtain (via online recruitment, for instance), the legitimate banking account information of an actual individual. Once this account information has been obtained, the subject can then create fraudulent checks that purport to be issued by various companies or individuals, and made payable to the individual whose account information the subject is in possession of. Once those fraudulent checks have been created, the only remaining step is to deposit those checks into ATMs, and using the ATM card and PIN of the recruited individual, subsequently withdraw the cash the bank credits to that recruited individual's account. Banks typically make at least $200 instantly available for withdrawal upon the ATM-completed deposit of a check or money order that purports to be for that amount or greater. Accordingly, this type of fraudulent activity, while perhaps limited only to that initial $200 return, is consistently successful and often times much more so.

27. Based on the above, the affiant submits that there is reason to believe that Device 1, Device 2, Device 3, and Device 4, Device 5, Device 6, Device 7 and Device 8 may contain further evidence of criminal activity to include evidence, fruits and instrumentalities of violations of Title 18 USC § 1349 (Conspiracy to Commit Bank Fraud) and 18 USC § 1028A(a)(1) (Aggravated Identity Theft).

28. Device 1, Device 2, Device 3, and Device 4, Device 5, Device 6, Device 7 and Device 8 are currently in storage at the Chesterfield County Police Property and Evidence Unit located at 9221 Public Works Road Chesterfield, VA 23832.

29. In my training and experience, I know that the devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the devices first came into the possession of the Chesterfield County Police.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

30. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

31. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few

examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

e. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and "chat" programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file

systems can record information about the dates files were created and the sequence in which they were created.

f. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

g. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but

not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

34. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

35. Based on the above, the affiant submits that there is reason to believe that Device 1, Device 2, Device 3, and Device 4, Device 5, Device 6, Device 7 and Device 8 may contain further evidence of criminal activity to include evidence, fruits and instrumentalities of violations of Title 18 USC § 1349 (Conspiracy to Commit Bank Fraud) and 18 USC § 1028A(a)(1) (Aggravated Identity Theft).

SPECIFICITY OF SEARCH WARRANT RETURN AND NOTICE REGARDING INITIATION OF FORENSIC EXAMINATION

36. Consistent with the Court's current policy, the search warrant return will list the model(s) and serial number(s) of any and all computers seized at the SUBJECT PREMISES, and include a general description of any and all associated peripheral equipment that has been seized. Additionally, the search warrant return will include the total numbers of each type of digital media that has been seized (e.g., "ten (10) 3.5" diskettes; twenty (20) CDs; twenty (20) DVDs; three (3) USB drives; one (1) 256 MB flash memory card," etc.)

CONCLUSION

37. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

TFO

Michael S. Bowser
Detective/Task Force Officer
United States Secret Service

Subscribed and sworn to before me
on May 29, 2018

/S/
David J. Novak
United States Magistrate Judge

David J. Novak
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is:

an Black ZTE cell phone, model Sky MM8005, S/N 325769982688;

an Red and white iPhone Model 1660 FCC ID BCG-E3085A, cracked screen;

White iPhone S Model A 1688 FFC ID BCG-E2946A, cracked screen;

Black Dell Laptop Model P28F S/N 276662519917;

an Gray HP Laptop with purple diamond sticker, Model 2000-369WM, S/N 53B218W2Y;

a Black IST Discover Flash Drive;

Black Coolpad Cellphone – Model 5560S,MEID (DEC) 256691536606894695, MEID (HEX) – 99000526693467, cracked screen;

Black iPhone – Model A1784, FCC ID: BCG-E3092A, IC: 579C-E3092A, cracked screen.

The property is collectively referred to as "The Devices."

The Devices are currently located at the Chesterfield County Police Property and Evidence Unit located at 9221 Public Works Road Chesterfield, VA 23832.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18 USC § 1349, and Title 18 USC § 1028A(a)(1), and involve WILLIAM REED, including:

a. Electronically stored data, files or digital information relating to violations of 18 U.S.C. § Section 1349, and Title 18 USC § Section 1028A(a)(1), stored on the computer hard drive of "Device 4" and "Device 5" as well as stored data, files or digital information stored on wireless phones of "Device 1", "Device 2", "Device 3", and "Device 7", and "Device 8" and flash drive of "Device 6."

b. Deleted, altered, damaged, or corrupted data stored in the same areas as above.

c. Computer system information and file structure data.

d. Recovered Software to include system operations software and device management software.

e. Electronically stored information verifying ownership of the aforementioned computer system and associated software including registration information.

f. Any records, notes, passwords or personal identifications (PINs), names, addresses, telephone numbers, account numbers, correspondence, email, chat logs relating to the aforementioned violations.

g. Any websites, newsgroups, or social media postings that describe obtaining or exchanging stolen credit card or bank account information.

h. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet Protocol address used to communicate with the internet, including:

a. records of Internet Protocol addresses used;

b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.